



DPC: 24/30479655 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 26 November 2024

Origin: International

Latest date for receipt of comments: 19 January 2025

Project No. 2023/02081

Responsible committee: IDT/1 Document Management Applications

Interested committees:

Title: Draft BS ISO 15801 Document management — Electronically stored information — Requirements for trustworthiness and reliability.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 19 January 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 15801

Document management — Electronically stored information — Requirements for trustworthiness and reliability

*Gestion de document — Information stockée électroniquement
— Exigences pour contribuer à l'intégrité et à la fiabilité des
informations stockées*

ICS: 35.240.30

ISO/TC 171/SC 1

Secretariat: **BSI**

Voting begins on:
2024-11-26

Voting terminates on:
2025-02-18

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/DIS 15801:2024(en)

Full document details: 24/30479655 DC

© ISO 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Scope of the ESI system	2
4.1 General	2
4.2 Risk management	2
4.3 Requirements	2
4.4 Boundaries and applicability	3
5 Policies and procedures	3
5.1 Policy requirements	3
5.2 Policy statements	4
5.2.1 General	4
5.2.2 Information storage policy statement	4
5.2.3 ESI transfer policy statement	6
5.2.4 Information security policy	7
5.2.5 Information classification	8
6 Roles and responsibilities of workers	9
7 Business environment	10
8 Operational procedures	11
8.1 Information management objectives	11
8.2 Actions to address risks and opportunities	11
8.2.1 General	11
8.2.2 Risk assessment	12
8.2.3 Risk treatment	12
8.3 Support	13
8.3.1 Resources	13
8.3.2 Competence	13
8.3.3 Awareness	13
8.3.4 Reporting	14
8.4 Documentation	14
8.4.1 General	14
8.4.2 Procedural documentation	15
8.4.3 System description	16
8.4.4 Audit trails	17
9 Operational procedures	18
9.1 General	18
9.2 ESI creation	18
9.3 Importing of ESI	19
9.3.1 General	19
9.3.2 Format conversion	19
9.3.3 Dynamic data files	20
9.3.4 Information loss	20
9.3.5 Internet of Things	20
9.4 Business process management, robotic process automation and workflow systems	21
9.5 Document scanning	21
9.6 Information extraction	22
9.6.1 Character recognition	22
9.6.2 Electronic forms	23
9.7 Metadata capture	23

9.8	Self-modifying files.....	23
9.8.1	Data files.....	23
9.8.2	Executables in databases.....	23
9.9	Compound documents.....	24
9.10	ESI in structured databases.....	24
9.11	Big data considerations.....	24
9.12	Blockchain and distributed ledger technologies.....	24
9.13	Version control.....	25
9.14	Storage systems.....	25
9.14.1	Storage technology.....	25
9.14.2	Migration.....	26
9.14.3	Storage file formats.....	27
9.14.4	Conversion.....	27
9.14.5	Compression.....	27
9.15	ESI transfer.....	28
9.15.1	General.....	28
9.15.2	Transmission.....	28
9.15.3	Message transmission systems.....	29
9.16	Indexing and other metadata.....	29
9.17	Authenticated output procedures.....	29
9.18	Identity.....	30
9.19	ESI retention, redaction and disposal.....	30
9.19.1	Retention.....	30
9.19.2	Redaction.....	30
9.19.3	Disposal.....	31
9.20	Information security procedures.....	31
9.20.1	General.....	31
9.20.2	Access control.....	32
9.20.3	Encryption.....	32
9.20.4	Digital signatures.....	32
9.20.5	Back-up and recovery.....	32
9.20.6	Business continuity plans.....	33
9.21	System maintenance.....	33
9.22	External service provision.....	33
9.22.1	Procedures.....	33
9.22.2	Compliance.....	33
9.22.3	Security in transfer.....	33
9.22.4	Overseas service provision.....	34
9.23	Information management system testing.....	34
10	System performance.....	34
10.1	General.....	34
10.2	Audits.....	35
10.2.1	Audit requirements.....	35
10.2.2	Audit objectives.....	35
10.3	Management review.....	35
10.4	Corrective actions.....	36
10.5	Continual improvement.....	37
	Bibliography.....	38

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 1, *Quality, preservation and integrity of information*.

This fourth edition cancels and replaces the third edition (ISO/TR 15801:2017), which has been technically revised.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Information is an organizational asset that needs to be appropriately managed throughout its lifecycle. Ensuring that the organization is able to demonstrate the trustworthiness and reliability of electronically stored information (ESI) is a key consideration. Failure to do so could result in non-compliance, loss of evidential value for information used in business, dispute resolution or legal proceedings.

This document specifies how ESI is to be managed by an organization in an information management system, to enable the organization to demonstrate the trustworthiness and reliability of the ESI throughout its lifecycle.

This document is for use in business, compliance, legal or other dispute resolution purposes, where the retained ESI needs to be relied upon to be exactly what it purports to be. This document will be useful for managers and professionals involved in management and governance of data, information, records, knowledge, digital preservation or e-discovery; and for the designers, vendors and operators of the information management systems that create, receive, store, transmit, preserve and dispose of ESI. It would also benefit the academic community and general public.

Where an organization conforms to this document, it is anticipated that the weight of evidence of ESI managed by the system will be maximized by ensuring its trustworthiness and reliability. This is likely to reduce the effort and cost involved in dispute resolution as the focus of the resolution process will be less concerned with the trustworthiness or reliability of disclosed ESI.

It is also anticipated that conformity with this document will minimize the risks involved with the credibility of ESI retained for the long term.

ESI originates from many sources. This document covers ESI in any form, from traditional scanned images, word processed documents and spreadsheets to the more “modern” forms which include e-mail, web content, instant messages, CAD drawing files, blogs, wikis, audio files, pictures and video. Also included is ESI stored in databases, Internet of Things (IoT) systems, distributed ledger technology (including blockchain systems) and other data storage systems (including the use of cloud storage).

When ESI preservation is considered, the requirements of ISO 14641 can be used in conjunction with this document. Readers are advised to use this document in conjunction with relevant authoritative sources in their respective jurisdictions, specifically for the purposes of compliance with applicable laws and regulations.

Document management — Electronically stored information — Requirements for trustworthiness and reliability

1 Scope

This document specifies the implementation and operation of information management systems that store and make available for use electronically stored information (ESI) in a trustworthy and reliable manner. Such ESI can be of any type, including “page based” information, information in databases and audio/video information.

This document is for use by any organization that uses information management systems to store trustworthy ESI over time. Such systems incorporate policies, procedures, technology and audit requirements that ensure that trustworthiness of the ESI is maintained.

This document does not cover processes used to evaluate whether ESI can be considered to be trustworthy prior to it being stored or imported into the system. However, it can be used to demonstrate that, once the electronic information is stored, output from the system will be a true and accurate reproduction of the ESI.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12651 (all parts), *Electronic document management — Vocabulary*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 electronically stored information (ESI)

information of any kind and from any source, whose temporal existence is evidenced by being stored in or on any electronic medium

Note 1 to entry: ESI includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. ESI also includes system, application and file-associated metadata such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, storage devices and storage elements.

[SOURCE: ISO/IEC 27040:2015, 3.16]

3.2

information type

groups of related information

Note 1 to entry: In specific applications, “groups” can be identified as “sets”, “files”, “collections” or other similar terms.

EXAMPLE Invoices, financial documents, data sheets, correspondence.

3.3

trustworthiness

ability to demonstrate authenticity, integrity and availability of ESI over time

4 Scope of the ESI system

4.1 General

The organization shall also determine the scope and requirements for the ESI system with respect to trustworthiness and reliability.

In order to ensure that ESI is well managed, and to meet its business needs, the organization should define and implement good management practices. ESI, like any other asset, should be classified, structured, validated, valued, secured, monitored, measured, managed and disposed of, when appropriate, efficiently and effectively.

All ESI used by an organization that is within the scope of the ESI system should be classified into “information types”. This classification should be used in the creation of policy statement(s).

NOTE For further information on classification, see ISO 4669 series

Increasingly, ESI is being sent from one electronic system to another, either within an organization or between organizations. The manner in which this movement of ESI occurs can determine the success or failure of the organization; thus, transfer systems should be secure, structured and auditable.

4.2 Risk management

A risk management process shall be used to identify the scope and requirements that are relevant to the trustworthiness and reliability of ESI.

NOTE 1 Typical scope and requirements that might be relevant include:

- a) the size and complexity of the organization;
- b) the level of business risk attached to being unable to demonstrate trustworthiness and reliability of ESI;
- c) drivers for business efficiency improvements;
- d) specific stakeholder requirements; and
- e) the existing technology and infrastructure systems.

NOTE 2 The risk management processes defined in ISO 31000 might be appropriate.

4.3 Requirements

When determining ESI management requirements, legal and regulatory requirements, duty of care, contractual obligations, business requirements and ESI stewardship throughout the ESI lifecycle shall be included. This should include:

- a) stakeholders that are relevant to the trustworthiness and reliability of ESI;
- b) the requirements of these stakeholders relevant to that ESI; and

- c) the requirements for information stewardship within the organization.

The requirements of each stakeholder should be taken into consideration when producing policy statements (see [5.2](#)).

Information stewardship should be managed by the identification of Information Asset Owners (IAOs) who are typically those responsible for the processes that manage the ESI asset in question.

4.4 Boundaries and applicability

When determining the scope of the information management system, the scope and requirements of the ESI system shall be taken into account. Where only part of the ESI held by the organization is included (for example, a single department or a single process could be defined as the scope of the system), the scope of the system shall be documented as part of the policy statement (see [5.2.2](#) and [5.2.3](#)).

When determining this scope, the organization should consider:

- a) the scope and requirements referred to in [4.1](#);
- b) the requirements referred to in [4.3](#); and
- c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope should be available as part of the policy statement(s).

In many organizations, the trustworthiness and reliability of ESI could only be of importance to part of the overall ESI asset. Individual ESI assets should be identified and a decision should be taken as to whether each is to be included within the scope of the related policy.

5 Policies and procedures

5.1 Policy requirements

The organization shall set a clear policy direction and demonstrate support for, and commitment to, the management of ESI that is within the scope of the system (see [4.1](#)) through the issue and maintenance of a policy covering the management of ESI.

The policy shall address the whole lifecycle of the referenced ESI and shall identify the role of the information steward(s) responsible for the referenced ESI at each stage of the lifecycle.

NOTE 1 The information stewardship may be transferred between individuals at different stages in the lifecycle of an ESI asset. This continuity of stewardship is important to demonstrate an unbroken chain of management and accountability throughout the life of the ESI.

The policy shall cover:

- a) the storage of electronic information (see [5.2.2](#)); and
- b) the transfer of ESI between systems (see [5.2.3](#)).

The policy shall be linked to or combined with the information security policy of the organization (see [5.2.4](#)).

NOTE 2 In some organizations this is called an information risk management policy.

The policy shall be published and communicated to all appropriate workers.

The policy shall have a custodian, responsible for its maintenance and review in accordance with the approved review procedure of the organization.

The policy shall be integrated into the processes of the organization.

Sufficient resource shall be available to implement the policy and to ensure the relevant outcomes are achieved and, where appropriate, improved.

The policy shall be documented in one or more policy statements.

5.2 Policy statements

5.2.1 General

A procedure shall be established to ensure that the policies covering the management of ESI are reviewed at regular intervals, and when any significant changes occur to the appropriate business, legal and/or regulatory environment.

NOTE 1 The review period is typically the same as the normal procedural audit cycle within the organization, for example, annual or in the event of major changes to the system.

The policy statements should set out guidelines for the appropriate application of an electronic identity for each document type. These statements should include the organizational requirements for identity, authority and copyright protection.

NOTE 2 The underlying issue with these items is the requirement to understand the significance of an electronic identity attached to a document. If it is always someone within the same organization, it is significantly less complex than between organizations because the organization can set its own rules. For all inter-organizational documents controlled with electronic signatures or copyright protection, it is imperative that the recipient organization is capable of understanding the significance of what is communicated to it, recognizing, implementing and utilizing the relevant controls.

This document also specifies the contents of an information security policy within which the information storage policy operates. The information security policy statement should document the level and rigour of protection required, detailing the requirements for each document type.

Where there is a requirement, the policy statements should describe the degree of security required, for example, some documents are not as significant as others and proof of the identity of the signatories is of less importance – for instance, an internal memo as opposed to a contractual commitment.

Approved policy statements should be retained in compliance with the retention schedule (see [9.19.1](#)).

5.2.2 Information storage policy statement

5.2.2.1 Structure

The information storage policy statement shall state the management commitment to, and approach for, the use of electronic systems in the storage of ESI over time in a controlled manner, taking account of the need to preserve the trustworthiness and reliability of the ESI.

Availability of this documentation should, when combined with appropriate proof of compliance, demonstrate (e.g. to a court of law) that responsible information storage is part of the normal business practice of the organization.

The information storage policy statement should be approved by the organization, and should be reviewed for relevance and content at regular intervals. The frequency for review should be appropriate to the application.

The policy statement shall, as a minimum, include the following elements or, where applicable, reference separate documentation on:

- a) the scope of the policy;
- b) the application of any applicable security classification to ESI (see [5.2.5](#));

- c) the implementation of various international and national standards and industry-related requirements and guidelines;
- d) the compliance with the policy of the organization for capture and retention of information;
- e) the definition and allocation of roles and responsibilities (see [6](#));
- f) any consultations that the organization needs to undertake (see [7](#));
- g) the use of the appropriate ESI storage technology (see [9.14.1](#));
- h) the use of the appropriate ESI file formats (see [9.14.3](#));
- i) the use of compression technology (see [9.14.5](#));
- j) the management of the linking of electronic identity to ESI (see [9.18](#));
- k) the capture, retention and disposal of ESI, including the management of temporary halts to the destruction of specific ESI (see [9.19](#));
- l) the use of encryption technology (see [9.20.3](#));
- m) the auditing of the information management system (see [10.2](#)).

NOTE Other elements may be included.

5.2.2.2 Scope

The policy statements described in [5.2.2.1](#) might not cover all the different types of ESI that the organization uses. The ESI to be included in its scope should be identified and grouped into types, with the policy for all ESI within a type being consistent. Where a retention schedule and disposal procedures (see [5.2.2.3.3](#)) exist, it might be appropriate to use the same ESI type groups.

Where formal records management procedures are implemented, ESI types will generally be used in classification schemes (file plans) and/or taxonomies. Where this is the case, the same file grouping and naming conventions should be used.

NOTE ESI types can be specified by reference to application (e.g. “financial projections”, “invoices” or “customer address list”) or by reference to generic group (e.g. “accounting data”, “customer documents” or “manufacturing documents”).

All applicable ESI types should be included in the policy statements.

An alternative to this approach of including only identified ESI types in the policy scope can be adopted, since there is a risk that the organization might need to produce absolutely any of its ESI assets in the event of a dispute. The organization should consider whether it needs to have any ESI that is totally unmanaged, even the ESI that is regarded as of very low value to the organization.

In this case, it is worth considering whether the policy scope should include a “default” ESI type (with associated policy and policy implementation and compliance requirements) as well as the explicitly identified ESI types. ESI outside the scope of the explicitly identified types should be managed according to the default.

5.2.2.3 Standards related to ESI management

Frequently, business benefits can be achieved by complying with relevant national or international standards, codes of practice or other guides. The policy statements should state whether all or specific parts of any such publication(s) are to be complied with.

NOTE 1 The ISO/IEC 27000 series of international standards are the reference documents for information security management.

Where the organization operates a quality management system (such as one in accordance with ISO 9001), whose scope includes part or all of the information management system within the scope of compliance, then all documentation that this document requires should be included in the quality management system.

Where information classification systems are used within the system, reference to ISO 4669-1 which includes requirements for the subsequent marking and handling of the classified information is advised.

5.2.3 ESI transfer policy statement

There are many forms of technologies and procedures that can be used for ESI transfers. The ESI transfer policy statement should give guidelines on the type of transfer technology to use in particular circumstances, on the content and layout of unstructured transfers and on the identification of the appropriate systems to be used for all corporate ESI transfers. In particular, the use of structured and unstructured forms of ESI transfers should be included.

Where unstructured or structured ESI transfers are involved, corporate guidelines on message structures should be included within the ESI transfer policy statement, or referenced by it.

The ESI transfer policy statement shall state the management commitment to, and approach for, the use of electronic systems for the transfer of ESI in a controlled manner, taking account of the need to preserve the trustworthiness and reliability of the ESI.

The ESI transfer policy statement shall include, as a minimum, the following elements or, where applicable, reference separate documentation on:

- a) the scope of the ESI transfer policy [which might be different from that for information storage (see [5.2.2](#))];
- b) the definition and allocation of roles and responsibilities for ESI transfer (see [5.2.3](#));
- c) the transfer of specific types of ESI (see [9.15](#));
- d) the use of data compression (see [9.14.5](#));
- e) the use of particular systems for the transfer of ESI (see [9.15](#));
- f) the receiving of transferred electronic ESI (see [9.15](#));
- g) the management of the linking of electronic identity to ESI (see [9.18](#));
- h) the use of encryption (see [9.20.3](#));
- i) the auditing of the ESI communication system (see [10.2](#)).

NOTE Other elements may be included.

The critical procedural issues are related to the delivery of and the receipt of ESI transfers, thus the ESI transfer policy statement should give guidelines on how these procedures are to be developed, and to what standards, including where ESI transfers are sent and/or received. These procedures (which may be different for send and receipt) should include:

- a) the avoidance of messages with illegal content;
- b) the avoidance of copyright issues;
- c) protection against malicious software;
- d) appropriate security procedures;
- e) the application of the organization's retention and disposal policies;
- f) the avoidance of spam and other inappropriate messages (incoming and outgoing); and
- g) the capture of audit trail evidence of transfer send and receipt.